MIND THE GAP

Weathering the Statutory Notification Process When a Data Breach Occurs

By John Garaffa and Matt Peaire

Even before Edward Snowden and the NSA entered into the public conversation, data breach concerns abounded. For instance, a recent study conducted by the Ponemon Institute surveyed 4,774 IT and IT security professionals from nine countries—U.S., UK, France, Germany, Japan, China, India, Australia, and Brazil—and revealed that 60 percent of companies had a network security breach in the last year and 34 percent of those companies experienced more than one breach.

The report also noted that 51 percent of companies struggle to prevent cyberattacks against their networks, and 61 percent reported that existing security technologies don't address the complete threat. For the business that stores its customers' personal information, the odds are that, at some point, it will experience a breach of its data storage system.

When a data breach occurs, the focus will necessarily be twofold. The company must determine the scope and nature of the breach and address both the potential danger to customers and the steps needed to avoid losing them to a competitor. While the internal response will depend on the unique circumstances of each company's data systems, the focus of the response for customer risk will be governed by state statutes.

Almost every U.S. state, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have statutes that specifically identify what a business must do in response to a potential data breach. Let's identify those statutes and discuss how various states address notification requirements following a potential data breach.

Depending on the scope of the exposure posed by the data breach, the potential cost of compliance can be a significant loss. The total cost of cybercrimes for 2010 was $388 billion, according to Norton's 2011 Cyber Crime Report, and the costs associated with investigating and remedying a breach of personal information were calculated at $194 per record, according to the Ponemon Institute.

The scope of personal information loss that will require notification of affected parties is defined by statute. For example, Montana's data breach statute defines "personal information" as follows:

> (b)(i) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
>
> (A) Social Security number;
>
> (B) Driver's license number, state identification card number, or tribal identification card number;
>
> (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

As commercial insurance policies continue to evolve, the standard commercial policy might not cover a data breach or cyber loss. Cyber policies can provide coverage that can both assist with the cost to address the mechanics of the data breach and help the business weather the significant cost of compliance with notification requirements. Close consultation with the business' insurance agent or broker can ensure that the business has the correct insurance in place when the time comes to respond to a data breach. A review of the data breach notification law for the jurisdiction will provide essential guidance on the scope of coverage required. (See Table 1 for the current statutes governing notification.)

Some state statutes have very thorough and potentially expensive notification requirements that differ depending on the size of the breach. The selection of the proper cyber insurance policy will govern whether the differing requirements imposed by the governing statute will be covered.

There are varied types of cyber policies with vastly different language concerning the scope of coverage. For

TABLE 1: STATUTES RELATING TO NOTIFICATION REQUIREMENTS FOLLOWING A DATA BREACH

STATE / TERRITORY	STATUTE(S)
Alabama	None
Alaska	AS § 45.48.010
Arizona	A.R.S. § 44-7501
Arkansas	A.C.A. § 4-110-105
California	Cal.Civ.Code § 1798.82
Colorado	C.R.S.A. § 6-1-716
Connecticut	C.G.S.A. § 36a-701b
Delaware	6 Del.C. § 12B-102
Florida	F.S.A. § 817.5681
Georgia	Ga. Code Ann., § 10-1-912
Hawaii	HRS § 487N-2
Idaho	I.C. § 28-51-105
Illinois	815 ILCS §530/10
Indiana	IC § 24-4.9-3-1
Iowa	I.C.A. § 715C.2
Kansas	K.S.A. § 50-7a02
Kentucky	None
Louisiana	LSA-R.S. § 51.3074
Maine	10 M.R.S.A. § 1348
Maryland	MD Code Commercial Law § 14-3504
Massachusetts	M.G.L.A 93H§3
Michigan	M.C.L.A. § 445.72
Minnesota	M.S.A. § 325E.61
Mississippi	Miss. Code Ann. § 75-24-29
Missouri	V.A.M.S. § 407.1500
Montana	MCA § 30-14-1704
Nebraska	Neb.Rev.St. § 87-803
Nevada	N.R.S. § 603A.220
New Hampshire	N.H. Rev. Stat. § 359-C:20
New Jersey	N.J.S.A. § 56:8-163
New Mexico	None
New York	McKinney's General Business Law § 899-aa
North Carolina	N.C.G.S.A. § 75-65
North Dakota	NDCC § 51-30-02
Ohio	R.C. § 1349.19
Oklahoma	74 Okl.St.Ann. § 3113.1
Oregon	O.R.S §646A604
Pennsylvania	73 P.S. § 2303
Rhode Island	Gen.Laws 1956 § 11-49.2-3
South Carolina	Code 1976 § 39-1-90
South Dakota	None
Tennessee	T.C.A. § 47-18-2107
Texas	V.T.C.A., Bus. & C. § 521.053
Utah	U.C.A. § 13-44-202
Vermont	9 V.S.A. § 2435
Virginia	VA Code Ann. §18.2-186.6
Washington	RCWA § 19.255.010
West Virginia	W.Va. Code § 46A-2A-102
Wisconsin	W.S.A. § 134.98
Wyoming	W.S.1977 § 40-12-502
District of Columbia	D.C. Code § 28- 3851
Guam	9 G.C.A. §48.30
Puerto Rico	10 L.P.R.A. §4052
U.S. Virgin Islands	14 V.I.C. §2208

Note: Current as of March 1, 2013

example, one policy defines covered "breach costs" associated with a data breach as "reasonable and necessary costs you incur…in response to a breach that triggers your notification obligations pursuant to any federal, state, local, or foreign statute or rule." That same policy defines "notification costs" as "legal costs, breach response call center costs, and costs to notify" the party whose information has potentially been the subject of the data breach. Other policies provide coverage for the costs related to investigating which customer information has been stolen as well as the provision of credit protection services for the affected customers.

Regardless of the size of the company, the notification process required by law can make the loss or compromise of customer personal information through a data breach economically crippling. While the language of state notification statutes differs, the intent is the same. The affected business is to notify the potentially affected customer and do so as soon as possible. Some states, such as California, have very detailed statutory notification requirements. Other states, such as Pennsylvania, are more general. For example, Pennsylvania's Breach of Personal Information Notification Act requires:

> An entity that maintains, stores, or manages computerized data that includes personal information shall provide notice of any breach of security of the system following discovery of the breach of the security system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person…the notice shall be made without unreasonable delay.

The goal of the Pennsylvania statute for prompt notification is underscored by the use of the phrase "without unreasonable delay," and the identification of those to be notified as "any resident" whose personal information is "reasonably believed to have been accessed and acquired." Other statutes require the notification of any customer whose personal informa-

tion "may" have been compromised.

The language makes it clear that a company that has suffered a data breach is not permitted to wait until it has thoroughly researched the breach and identified which of its customers' information has been stolen. If a company has experienced a data breach, and it is not immediately apparent which of its customers' information has been compromised and which of its customers' information remains secure, the company will need to notify every customer of the potential breach. The expansiveness of the notification requirement and the expense of notification make coverage for the potential expenses a critical component of risk management.

State statutes reflect the respective legislatures' appreciation of the costs that might be associated with such a breach. Oregon's notification statute provides that, if the person or company demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of customers to be notified exceeds 350,000, notification can be done with a "conspicuous posting of the notice or a link to the notice on the Internet" and "notification to major statewide television and newspaper media." A similar provision in the North Carolina statute sets forth exactly what must be contained in the notice:

1. A description of the incident in general terms
2. A description of the type of personal information that was subject to the unauthorized access and acquisition
3. A description of the general acts of the business to protect the personal information from further unauthorized access
4. A telephone number for the business that the person may call for further information and assistance, if one exists
5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports
6. The toll-free numbers and addresses for the major consumer reporting agencies
7. The toll-free numbers, addresses, and website addresses for the Federal Trade Commission and North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.

State legislatures have responded to the danger posed by data breaches by enacting laws that require businesses to notify potentially affected customers as soon as possible.

While the statutory language from each state might not be the same exactly, the intent is clear. State legislatures have responded to the danger posed by data breaches by enacting laws that require businesses that suffer a breach to notify potentially affected customers as soon as possible. Under these statutes, businesses that suffer a data breach will not be able to take the time to determine exactly which of their customers have been exposed by the breach. Thus, the scope of the notification and its attendant costs can be extreme. For example, when Sony suffered an alleged breach connected with its PlayStation Network, it reportedly had 77 million customers, each of whom needed to be notified of the potential data breach.

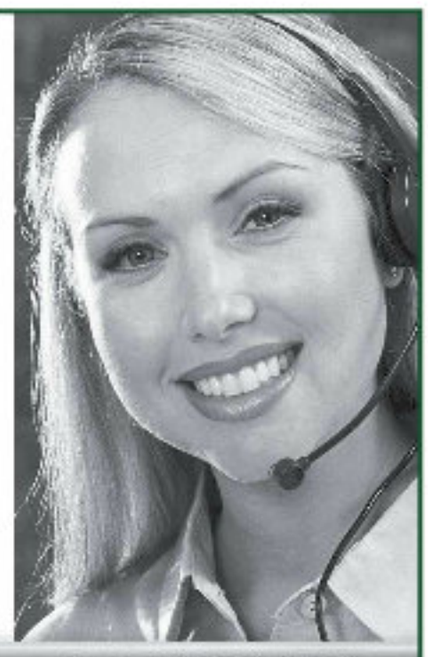
The investigation of a potential data breach may conclude that the breach was harmless or even that no loss of customer information was suffered. However, state statutes make it clear that businesses are to err on the side of caution and notify potentially affected customers as soon as practicable. This can be a costly process regardless of the eventual analysis of the actual data loss. This is a risk that can be covered by a cyber insurance policy that takes into consideration applicable state notification requirements. Businesses are, thus, well advised to have their risk managers review the state statute that would govern a data breach for their business to ensure they have the correct coverage in place. CM

John Garaffa and Matt Peaire are partners at the CLM member firm of Butler Pappas Weihmuller Katz Craig LLP. They can be reached at jgaraffa@butlerpappas.com, mpeaire@butlerpappas.com, respectively.

Are you looking for a permanent solution for temporary housing?

Experience the DMA Difference

- Immediate Hotel Stays
- National 24/7/365 Relocation Services
- Fully Furnished Housing
- Furniture Only Packages
- Property Rent Only Packages
- Travel Trailers



DMA
INSURANCE HOUSING ASSISTANTS

You can find out more about DMA Insuance Housing Assistants by calling us, toll free, at **1-800-550-1911** or by visiting us on the web at **www.dmahousing.com.**

Phone: 800.550.1911 • Fax 800.206.9425